







 rttbot / 

[Code](#) [Issues](#) [Pull requests](#) [Actions](#) [Projects](#) [Security](#) [Insights](#)

TICS0866-TALLER1-OWASPML / S6-2-01-acuerdo-hacking-etico.md 

...

 **rttbot** Update S6-2-01-acuerdo-hacking-etico.md 28c502d · 5 minutes ago  History

ACUERDO DE CONFIDENCIALIDAD Y HACKING ÉTICO

TICS00866: Auditoría y Defensa en Sistemas de Inteligencia Artificial

Documento: S5-4-00

Versión: 1.0

Fecha: Agosto 2025

TICS0866-TALLER1-OWASPML / S6-2-01-acuerdo-hacking-etico.md

[↑ Top](#)[Preview](#)[Code](#)[Blame](#)

143 lines (101 loc) · 5.39 KB

[Raw](#)

Entre:

Prof. Romina Torres

Cargo: Profesora Asociada Universidad Adolfo Ibáñez

Asignatura: TICS00866 - Auditoría y Defensa en Sistemas de Inteligencia Artificial

Y:

Estudiante: _____

RUT (NO INDICAR DADO QUE ESTO ES EJERCICIO ACADÉMICO):

Email: _____

Carrera: _____

Usuario GitHub: _____

OBJETIVO DEL ACUERDO

El presente acuerdo establece los términos y condiciones para la realización de actividades de **hacking ético** y **pentesting** en sistemas de inteligencia artificial como parte del Taller 1 de la asignatura TICS00866.

Descripción del Sistema

- **Nombre:** Intrusion.Aware
- **Propósito:** Sistema inteligente de detección de ataques cibernéticos mediante Machine Learning
- **Tipo:** Proyecto de investigación financiado por FONDEF-ANID
- **Institución:** Universidad Adolfo Ibáñez
- **Acceso:** Limitado al período del taller para fines educativos

Alcance del Análisis

- **Período:** 9 de septiembre de 2025
 - **Duración:** 2 bloques de 70 minutos (140 minutos total)
 - **Metodología:** Pentesting ético con técnicas de ataque adversarial
 - **Objetivo:** Diseñar casos de prueba para vulnerabilidades ML01-ML10 en Intrusion.Aware
 - **Modalidad:** Solo diseño de casos de prueba (NO implementación)
 - **Enfoque:** Explicar cada vulnerabilidad de IA de manera simple y comprensible
-

OBLIGACIONES DEL ESTUDIANTE

1. Confidencialidad

- **No divulgar** información técnica del sistema Intrusion.Aware
- **No compartir** credenciales de acceso al proyecto FONDEF-ANID
- **No documentar** detalles de implementación fuera del contexto académico
- **Mantener confidencialidad** de hallazgos del proyecto hasta autorización

2. Uso Ético

- **Solo diseñar** casos de prueba para Intrusion.Aware (NO implementación)
- **No realizar** ataques reales fuera del entorno controlado
- **No intentar** acceder a sistemas del proyecto FONDEF-ANID posterior a esto a menos que esté autorizado.
- **No divulgar** información entregada en el taller referente al proyecto posterior al cierre de este y a externos del curso.
- **Destruir** toda información entregada en el taller referente al proyecto cerrado el curso. No mantener información en su computador.
- **Reportar inmediatamente** cualquier incidente de seguridad solo a la profesora

3. Responsabilidad Académica y Social

- **Explicar de manera simple** cada vulnerabilidad de IA asignada
- **Documentar** todos los casos de prueba realizados
- **Entregar** reportes en los formatos establecidos
- **Participar activamente** en las actividades del taller
- **Respetar** los límites de tiempo establecidos
- **Contribuir** al objetivo de proteger a la sociedad de sistemas de IA inseguros

4. Cumplimiento Legal

- **Respetar** la legislación chilena vigente
 - **No realizar** actividades que puedan ser consideradas delictivas
 - **Actuar** dentro del marco legal y ético establecido
 - **Reportar** cualquier actividad sospechosa
-
-

TÉCNICAS/ACTIVIDADES PROHIBIDAS o NO PERMITIDAS

Actividades No Permitidas

- **Implementación real de ataques** al sistema Intrusion.Aware
- **Acceso no autorizado** a sistemas del proyecto FONDEF-ANID
- **Manipulación de datos** de otros estudiantes
- **Uso de herramientas** no autorizadas para el taller
- **Actividades que puedan causar daño** al proyecto de investigación
- **Subir documentación del proyecto a sistemas de IA generativa.**

Restricciones

- **No compartir credenciales** del proyecto FONDEF-ANID
 - **No realizar ataques reales** - Solo diseño de casos de prueba en este taller
 - **No documentar información sensible** del proyecto fuera del contexto académico
 - **No usar técnicas** no autorizadas para el análisis de Intrusion.Aware
-
-

FIRMAS Y FECHA

Estudiante:

Nombre: simon valenzuela

Firma: _____

Fecha: 09-09-25 _____

RUT: 20605363-1 _____

Profesora:

Nombre: Prof. Romina Torres

Firma: _____

Fecha: _____

Cargo: Profesora Asociada

Testigo:

Nombre: Julian Contreras _____

Firma: _____

Fecha: 09-09-25 _____

Cargo: Estudiante _____

DECLARACIÓN ADICIONAL

Declaro que he leído y comprendido completamente este acuerdo, y me comprometo a cumplir con todas las obligaciones establecidas para el análisis ético del sistema Intrusion.Aware del proyecto FONDEF-ANID. Entiendo que el incumplimiento de este acuerdo puede resultar en sanciones académicas y legales, y que debo mantener la confidencialidad de la información del proyecto de investigación.

Firma del estudiante: _____

Fecha: _____

Preparado por: Prof. Romina Torres

Fecha de preparación: Agosto 2025

Versión: 1.0

